Organised cybercrime or cybercrime that is organised? An assessment of financial cybercrime as organised crime

Leukfeldt, E.R.; Lavorgna, A.; Kleemans, E.R.

published in
European Journal on Criminal Policy and Research
2017

DOI (link to publisher)
10.1007/s10610-016-9332-z

document version
Early version, also known as pre-print

Eur J Crim Policy Res
DOI 10.1007/s10610-016-9332-z

Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime

E. Rutger Leukfeldt[1] **· Anita Lavorgna**[2] **· Edward R. Kleemans**[3]

Abstract Criminological research over the last couple of decades has improved our understanding of cybercrimes. However, this body of research is regarded as still theoretically thin and not fully developed; more knowledge on the actors involved, their characteristics, and modus operandi is needed. Some publications recently suggested that organised crime is or might be involved in cybercrimes, which would have important policing implications, but evidence-based research on this point is still scarce and inconclusive. This article seeks to further this path of inquiry by providing a systematic analysis of 40 cases from The Netherlands, Germany, UK, and USA where criminal networks were involved in financial cybercrimes affecting the banking sector. It also assesses whether and to what extent these criminal networks meet the definitions of organised crime and discusses the theoretical and policing implications of our findings.

Keywords Organised crime · Cybercrime · Phishing · Malware · Financial crime

Introduction

With the Internet becoming embedded in countless aspects, routines, and practices of today's way of living; connectivity is now an established feature of our society (Hassan 2008). The same features that have consolidated the success of the Internet, however, are also criminogenic and have led to new offences that are enabled or enhanced by technologies—

✉ Anita Lavorgna
A.Lavorgna@soton.ac.uk

[1] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan 1077a, 1081 HV Amsterdam, The Netherlands

[2] University of Southampton, Murray Building, 58 Salisbury Rd, Southampton SO171BJ, UK

[3] Vrije Universiteit Amsterdam, De Boelelaan 1105, 1081HV Amsterdam, The Netherlands

Published online: 12 November 2016

so-called cybercrimes (Choo et al. 2007; Wall 2007). Criminological research over the last couple of decades has improved our understanding of cybercrimes, with a substantial number of studies expanding our knowledge on both offending and victimisation (for a recent review of the literature, see Holt and Bossler 2014). However, this body of research is regarded as still theoretically thin and not fully developed (Lagazio et al. 2014).

One major problem is that the concept of cybercrime is complex, and it encompasses an extremely broad range of different crimes; some can be assessed through an economic perspective, while others are motivated by ideology, passion and even revenge. For analytical precision and to limit potential research bias, as different types of offenders are likely to be involved in different types of cybercrimes, in this study, we focus only on profit-driven cybercrimes affecting the banking and financial sector as well as specifically phishing and malware attacks.[1] These types of crimes have become increasingly problematic over the last 15 years, with the advent of online banking and the proliferation of electronic funds transfer systems (Smith 2010: 223ff). It is difficult to assess their impact, and both financial costs and intangible losses (such as reduced customer trust) can be acknowledged (Wall 2008; Lagazio et al. 2014). Estimates are impressive, with a cost of almost £2.5 billion in the UK alone (Cabinet Office and Detica 2011), even if it has to be stressed that these estimates have been criticised because of their low level of reliability (Kshetri 2010).

In order to better counter these types of criminal activities, more knowledge on the actors involved, their characteristics, and modus operandi is needed. Some publications suggested that organised crime (hereafter, OC) is or might be involved in financial cybercrimes (to name a few, Williams 2001; Birk et al. 2007; Grabosky 2015), which would have important policing implications, but evidence-based research on this point is still scarce and inconclusive. When it comes to criminal networks active in cyberspace, in fact, some researchers are increasingly adopting the OC narrative to describe a broad range of offenders (for instance, Choo and Smith 2007; McGuire 2012). Others, on the other hand, are more cautious in expanding the usage of OC in the absence of further understanding of the characteristics of these criminal networks, as OC is not an aseptic notion but has a strong, evocative power (Lusthaus 2013; Lavorgna 2016). This article seeks to further this path of inquiry and contributes to this debate by presenting empirical research: the section "Cyber OC: success and criticism of a concept" provides a focused literature review on the presence of OC groups in cyberspace; the section "Data gathering and analysis" describes data and the methods used in this study; sections "Empirical results" and "Discussion" focus on the composition and structure of the cybercriminal networks analysed, their social relationships, use of violence and corruption and connections with the legal economy. We then assess to what extent such relationships meet the current definitions of OC. Finally, Section "Implications and conclusion" discusses the theoretical and policing consequences of our findings and suggests topics for further research.

Cyber OC: Success and Criticism of a Concept

A growing number of academic studies and reports from cybersecurity companies show that varieties of organisational structures are involved in cybercrimes and have expanded the notion

[1] Phishing can be defined as "a scalable act of deception whereby impersonation is used to obtain information from a target using digital means such as email" (Lastdrager 2014). Malware (malicious software) are programs used to compromise computer systems and steal information.

of OC to cover profit-driven criminal phenomena occurring completely or partially in cyberspace (Williams 2001; Choo and Smith 2007; Grabosky 2007; Broadhurst et al. 2014). Regarding financial cybercrimes specifically, Birk et al. (2007) referred to organised cybercrime in cases of identity theft through phishing, but organisational structures are not analysed in their study. More recently, Hutchings' study on computer crimes compromising data and financial security (Hutchings 2014) suggested that many cyber offenders are highly networked, cooperate with each other to commit offences, and learn their behaviour from others. The results, however, are not conclusive for indicating whether we should label these groups operating online as OC. A widely quoted report is that from BAE Systems Applied Intelligence on the use of information and communication technologies (ICTs) by organised criminals (McGuire 2012). The report identified three main types (type I, II, and III) and six subtypes (swarm, hubs, extended hybrids, clustered hybrids, aggregates, and hierarchies) of cyber OC groups and concluded that up to 80 % of cybercrime is OC. According to the report, certain key characteristics of traditional OC groups need to be reconsidered when groups are operating online: for instance, in cyberspace, the size of a group does not correlate with the impact and scope of offending, and many associations are highly transitory. The interpretation offered in the report is that cyberspace augmented, rather than replaced, existing varieties of organised criminal organisations. To decide whether a certain network of offenders should be labelled as OC, however, the report looked at recurring offending patterns and the scale of activity, overlooking the debates around the OC definitions and adopting the OC umbrella term to include a broad range of groups exhibiting some degree of organisation.

Similarly, the narrative used in policymaking often assumes a convergence between OC and cybercrime without strong empirical evidence (Lavorgna 2016; Lavorgna and Sergi 2016) but rather by relying on the "seriousness paradigm" of OC, which postulates an often unjustified juxtaposition of the seriousness of criminal activities and the organised character of criminal actors (Sergi 2015a). As already stressed by Lusthaus (2013), Lavorgna (2015, 2016), Leukfeldt (2015), and Wall (2015), among others, there is not enough consistent and solid evidence to make analogies between cybercrime groups and OC.

With reference to "offline" crimes, the very low standards that have been set for inclusion of different and diverse phenomena such as OC have been severely criticised in academia. OC is often accused of as being used as "a catchphrase to express the growing anxieties" on the expansion of illegal markets and the perceived growing undermining of the legal economy and political institutions (Paoli 2002: 51). Also, ambiguities around the notion of OC have reportedly been used for producing consensus around increased resources, domestic powers, and international cooperation in policymaking (Edwards and Levi 2008; Carrapico 2014), as defining a group of offenders as being OC orientates policing responses by allowing more resources and investigative power (Van Duyne 2004; Levi 2014). However, the presence of conceptual inconsistencies (or "paradoxes" in the words of Paoli 2002) and ongoing definitional debates hinder the construction of a conceptual and analytical framework to forge advancements in both policing and research (van Duyne 1995, 2004; Van Duyne and Nelemans 2012; Carrapico 2014). OC experts, in contrast with the very low standards set in policymaking, tend to refine the notion of OC to something more and different than just crime that is organised (Schelling 1971; von Lampe 2008; Allum et al. 2010; Varese 2010): as summarised by Lusthaus (2013), OC is also a form of governance within the criminal world.

Our study proposes to advance the debate on the extent to which cybercrime is OC by providing a systematic analysis of 40 cases from The Netherlands, Germany, UK, and USA where criminal networks were involved in financial cybercrimes affecting the banking sector.

It assesses whether and to what extent these criminal networks meet existing definitions of OC and discusses the theoretical and policing implications of our findings. Indeed, as the threatening aspects of OC in public debates are related to elements of these traditional, existing definitions, it is important to "test" with empirical data to what extent these elements are present in (our considered subset of) cybercrimes.

Data Gathering and Analysis

Data was gathered in the context of the doctoral research of ERL and the Dutch Research Programme on Safety and Security of Online Banking from criminal investigations into cybercriminal networks in The Netherlands, UK, USA, and Germany (for further details, see Leukfeldt et al. 2016a, b, c).

In the Netherlands, the researcher had access to 18 police investigation files, which provided unique knowledge because of the wide-ranging use of investigative methods, such as wiretaps and IP taps, observation, undercover policing, and house searches. For the purposes of this research, only investigations into criminal networks that the police had already "completed" were used, meaning cases for which the investigation team had collected enough evidence for the Public Prosecution Service to decide to prosecute, although a court judgment may not necessarily have been issued yet. Waiting for a court judgment, in fact, would have meant that only a few cases would have been available for analysis, as it can take years for suspects to be convicted (for a more extensive review of these methodological issues, see Kleemans 2014). There is no central registration system in The Netherlands that allows for a quick overview of all criminal investigations into phishing and malware networks. Based on existing contacts within the Dutch police, the Police Academy, and the Public Prosecution Service, the researcher asked team leaders and senior law enforcement officers whether they knew of any investigations into networks that used phishing or malware to attack users of online banking. In addition, he examined an online database of court documents (www.rechtspraak.nl) and carried out a media analysis in order to find news reports about relevant cases. This resulted in the identification of ten criminal investigations. The researcher asked law enforcement officers involved in the selected cases whether they knew of any other phishing or malware case, which resulted in a further eight cases. All investigations identified lasted for between 6 months and 3 years and occurred between 2004 and 2014. Semistructured, face-to-face interviews with the Public Prosecution Service, police team leaders, and senior detectives (including financial and digital experts) conducted between March 2013 and November 2014 complemented the document analysis of the criminal investigations.

In Germany, the UK, and the USA, the researcher had no direct access to police files. Instead, he reconstructed the characteristics of the cybercriminal networks from the basis of 28 interviews carried out between March 2014 and November 2015 with officers who investigated relevant criminal cases. By relying on existing contacts within the Dutch police (especially the Dutch High Tech Crime Unit) and the Dutch Police Academy, the researcher was able to access interviewees in the UK National Crime Agency, the United States Secret Service, and the German Bundeskriminalamt (BKA). In addition, wherever possible, official court documents about the cases were analysed. In total, the researcher gathered data for 22 cases: nine in the UK, ten in the USA, and three in Germany. The researcher also used open-

source information (e.g. news articles about the case) to complement the information provided by respondents. The 22 cases analysed covered the period 2003–2014.

In total, 40 investigative cases (and therefore 40 different criminal networks) were analysed for this study. Networks 1–18 were investigated in The Netherlands, networks 19–27 in the UK, networks 28–37 in the USA, and networks 38–40 in Germany. The selected cases were systematically analysed using the analytical framework developed and used by the Dutch Organised Crime Monitor, a long-running programme researching the nature of OC in The Netherlands (e.g., Kleemans 2014; Kruisbergen et al. 2012). The framework considers a number of key elements and characteristics generally associated with OC, such as composition and structure of criminal networks, social relationships, use of violence and corruption, and connections with the legal economy. While OC is conceptualised around the world in different ways (e.g., Albanese et al. 2003), the above-mentioned characteristics reflect the consensus concernng the main elements necessary for OC to be classified as such, as identified by the mainstream literature (Adamoli et al. 1998; Arsovska 2011; Tilley and Hopkins 2008). Other features—such as membership restrictions, secrecy, ideology, specialisation, presence of ethnic or cultural ties, and so on—are more controversial.

Empirical Results

Composition and Structure of Criminal Networks

None of the networks we studied had a strict hierarchical structure. This, however, does not mean that they were completely fluid; all networks displayed dependency relationships and different functional roles. Within the majority of networks in our analysis (30 of 40), three different layers could be recognised (Leukfeldt et al. 2016a, b, c): core members, enablers, and money mules. Core members initiated and coordinated attacks on financial institutions and directed other members of the network. Without these core members, the crimes could neither have been initiated nor committed. Enablers provided services necessary to execute the crime scripts (i.e., the series of steps needed to commit a crime). These criminals did not work solely for one particular network and advertised their illegal services online. Money mules were used to disguise the financial trail leading to core members. Some exceptions occurred in cases where core members did not need the services of enablers or did not use money mules. Money mules were easily replaceable, and criminal networks could use hundreds of them in their attacks. Therefore, they have not been included in the rest of the analysis if not otherwise specified. In the remaining ten cases, core members did not need the services of enablers or money mules to execute the crime scripts, as they already had all the necessary capacities.

We had in-depth information about core members for 27 networks. In most of cases (22 of 27), criminal networks consisted of a stable group of core members—meaning they committed crimes with the same composition over a period of time—who initiated and carried out attacks on financial institutions. Even when networks had a stable group of core members, however, individual core members often worked together with criminals from other networks. In the other five networks (without a stable group of core members), prior to the cyber attacks, criminals used online forums to look for other suitable co-offenders. In Network 34, for example, all core members had their own technical expertise (such as hacking, exchanging digital currency to real-world currency, and money laundering); they were all self-employed

entrepreneurs active individually on online criminal markets and who on occasion worked together.

The investigative cases analysed did not provide a ready-made picture of all members of criminal networks. However, they did provide a picture of the minimal number of criminals who worked together. We gathered information about the number of core members and enablers for 36 networks: there were two networks with only four criminals working together (small networks); 21 networks with between five and ten members (medium networks); 11 networks with between 11 and 20 members, and one network with more than 21 members (large networks). Network 21 is an example of a small network. The four core members had all been active in the criminal arena for a long time. They had met each other on chat boxes relating to coding, developed their own malware, used it to steal credentials from customers of financial institutions, and then sold these credentials on online forums. Because the core members had all the skills necessary for stealing the credentials, they did not have to rely on any enabler. Furthermore, there was no need for a large network of money mules (and people controlling these mules) to cash money, as these criminals sold the credentials to others instead of using the information themselves to attack individual customers of financial institutions. Network 18 is a typical example of a medium network. This Latvia-based network used malware to steal money from online bank accounts of victims in various European countries. The exact number of core members is unknown, but criminal investigations clarified that one core member developed the malware, while another coordinated the money transfers from the accounts of victims to the accounts of money mules. The core members used nine facilitators to recruit and control money mules. Some recruiters operated from Latvia and others from the countries of the victims. Another enabler forged the identity documents needed for money mules to open new bank accounts. An enabler working at the border control smuggled money mules from Latvia. Finally, Network 1 (large network), involved in phishing, had the largest number of core members and facilitators. The eight core members had different responsibilities, such as coordinating the transfer of money to the mules' accounts, recruiting new money mules, and cashing money from the money mules' accounts. The core members used phishing emails and websites to obtain login codes of online bank accounts. One core member contacted a friend abroad who had a friend that could make phishing websites; the core member gave him the order to make phishing websites for two banks. One of the enablers acted as a call centre agent to get one-time transaction codes from victims over the phone in order to transfer money from their online bank accounts. Furthermore, bank employees, postal workers, and cashers were involved in the execution of different parts of the crime script.

Social relationships

We obtained information on origin and growth of 39 networks and identified four types:

(I) Completely through offline social contacts;
(II) Offline social contacts as a base and online forums to recruit specialists;
(III) Online forums as a base and offline social contacts to recruit local criminals;
(IV) Completely through online forums (Leukfeldt et al. 2016a, b, c).

A total of 29 networks fell within the first two types, while only ten were part of the last two types and grew primarily using online forums. This means that offline social ties still play a crucial role in the origin and growth of cybercriminal networks. Core members, enablers, and money mules are recruited using existing social contacts; co-offenders, for example, usually grew up in the same neighbourhood, went to the same church or soccer club, knew each other from the criminal underworld, or met each other in prison. Offline social ties were particularly important in the origin and growth of networks with a stable group of core members: . Only in a couple of networks with a stable group of core members were these core members strangers who met on online forums and never had real-life contacts. The fact that offline social ties still matter does not mean that online forums are not important for cybercriminal networks. Even networks that relied primarily on offline social ties often did use online meeting places for recruiting specialised enablers, and purchasing or selling tools and services. Networks that relied mostly on forums for their origin and growth used them to meet other suitable core members, recruit enablers, and/or sell their criminal services or stolen personal data.

We also examined whether the networks from our analysis had ties with traditional offline OC groups: five of the 40 networks showed some evidence of this. For instance, Network 25 was a traditional OC group, with some members experimenting with high-tech crimes to make additional profits. The core members all had an active criminal career in London for many years. According to the police respondents, some core members were part of a well-known crime family involved in fraud, drug trafficking, money laundering, and racketeering. They recruited two hackers from another country to develop malware that allowed them to intercept and alter information of computers within a bank and then used their criminal contacts to set up bank accounts all over the world to transfer the money. In the four other networks, traditional OC groups provided services such as money laundering and access to fake identity documents. It is not known exactly how core members of cybercriminal networks and members of traditional OC networks got to know each other. Network 40, for example, was a Berlin-based group that carried out malware attacks on online banking sites; it relied on members of an outlaw motorcycle club to manage money mules (in the physical world). The core members of Network 24 had known each other from the criminal world in Vietnam; they were involved in hacking databases with credit card and debit card information, developing malware, and selling such information and services on forums to customers from all over the world. They used members of traditional Vietnamese OC as enablers to launder money: while cybercriminals usually pay using virtual currency, the enablers used a network of mule herders and money mules to cash the money.

In the 29 networks in which origin and growth occurred completely or primarily offline (types I and II), trust was a major factor explaining their origin and growth. As in traditional offline crime networks, pre-existing social relationships were essential to explaining why criminal cooperation started in the first place (Kleemans and Van de Bunt 1999; Leukfeldt et al. 2016a). Similarly, if we consider networks that mainly developed online (types III and IV), in most cases (8 of 10), trust was gained over a long period of time and, once it had been established, criminals tended to stick together: core members had been active for years in virtual communities; for instance, via chat boxes for coders or in forums used by hackers to exchange knowledge. These core members, who initially met each other online, jointly executed all sorts of cybercriminal attacks over time and used enablers when needed. However, in two cases, cooperation among core members and enablers was built ad hoc for specific cyberattacks, and trust was established in a different way: core members looked for

suitable co-offenders on dedicated forums designed specifically to facilitate these types of encounters. For instance, forum members had different statuses (ranging from newcomers to verified members), and ranking systems were used to rate the services they provided; furthermore, forum administrators tested some of goods and services and labelled them as "good" when only satisfactory. Hence, the opportunity structures to meet other reliable co-offenders and to quickly build a system of trust was provided by online forums (cf. Holt 2013; Yip et al., 2013). Prior analysis showed that networks that primarily used online forums for growth were able to perform international attacks with a relative small group of offenders (Leukfeldt et al. 2016b, c).

Use of Violence and Corruption

We found to cases with evidence of violence carried out by core members and/or enablers. In some cases, firearms were found during house searches, but they were not used in the commission of the crimes analysed. A handful of money mules stated that they cooperated because core members or enablers threatened them, but we do not know how reliable these statements are, as observations by police investigators, wiretapped phone calls, and Internet data do not back up these claims. Furthermore, none of the core members or enablers were indicted for violence.

Evidence of corruption was not found in any case. In ten cases, interviewees pointed out that some sort of involvement of Eastern European or Russian officials was likely to have occurred to explain the success of specific crime scripts. While police investigations provided no evidence of corruption, this absence may be because investigations focused on stopping specific and ongoing cybercrimes. Therefore, police may not have had time or resources to additionally investigate corruption.

Connections with the Legal Economy

In ten investigations, we found evidence of connections between cybercriminals and the legal economy. In three cases, bank employees working in banking call centres and postal workers were involved in the crime script. The bank employees provided core members with information about bank customers and their bank accounts that could be used in social engineering attacks, or they made unauthorised changes in the accounts of customers. Examples include increasing the limits of cash withdrawals (so fewer money mules had to be used to cash money) and changing addresses in such a way that postal workers who were working in certain areas were able to intercept the mail with new login codes of online bank accounts. In one case, the security manager of a bank helped criminals to physically get into the bank to place key loggers on computers. In three cases, there was evidence of money laundering through the creation of legitimate businesses in the physical world. In one case, the core members developed an online platform on which digital currency could be anonymously exchanged between members. This platform could be used for legitimate purposes, but criminal investigations revealed that this particular platform was popular among cybercriminals. When core members, for example, bought malware on a forum, payments had to be made using this online platform. Finally, it is worth noting that almost all networks analysed used legitimate money transfer services (such as Western Union) and digital currencies (such as eGold and Liberty Reserve) to make payments and manage their profits.

Discussion

Can the networks analysed in this study be conceptualised as OC? Overall, definitions of OC vary extensively, and there is not always a perfect correspondence between the various legal definitions and those used in policymaking and academia. Most legal definitions of OC tend to be broad, overarching several types of serious criminal activities and including a variety of different criminal groups: after all, defining a criminal network involved in illegal activities as OC suggests the existence of a whole mechanism to tackle, thus orienting responses of law enforcement and triggering greater investigative powers and tougher sentences in many countries (Levi 2014). Academic literature has already extensively criticised the "very loose and vague definitions" of OC adopted by legislators, which set extremely low standards for inclusions of different and diverse phenomena such as OC with the risk that "the concept might become an empty signifier" (Carrapico 2014: *11*).

As summarised by von Lampe (2008), when the notion of OC is boiled down, three different perspectives emerge. First, OC can be about the organisation when this notion denotes the presence of more or less stable and structured links among offenders. Second, OC can be about criminal activities characterised by a certain level of sophistication and continuity. Third, OC can be about the concentration of power, when the focus is on the presence of a systemic condition in the form of an underworld government or an alliance between criminals and political and economic elites (von Lampe 2008). Therefore, OC is not only ontologically different from opportunistic individuals, it also evokes the idea of an interpersonal and social threat. Because of this, it constitutes a bigger threat. The idea is that what individuals can do, organisations can do better (Lavorgna 2016).

If we only look at the composition and structure of criminal networks, most networks observed do meet the existing definitions of OC. As anticipated above, most legal definitions (and working definitions used by practitioners) tend to set very low standards—generally, the presence of a minimum of two or three persons working together over time (e.g., Potter 1994; Finklea 2010; Kruisbergen et al. 2012; Lombardo 2012; Sergi 2015a; Hobbs 2013; BKA 2014; Lavorgna and Sergi 2014), with differences depending on the specific conditions found in the areas where the groups emerged (Lavorgna et al. 2014). Similarly, criminological definitions of OC include a variety of phenomena—ranging from traditional and stereotypical Mafias to simpler criminal groups—and shift from overly narrow to overly broad definitions. Some meta-analyses of OC definitions suggest that a continuing, organised hierarchy remains a key trait of OC for many academics (Hagan 2006), However, others show that when OC is conceptualised in terms of collectives, these conceptualisations vary, and terminology (networks, organisations, groups, and so on) is often used in an intuitive, shallow sense. In this way, a wide variety of cooperation structures are encompassed under the umbrella term of OC (von Lampe et al. 2006), which might be the case with most of networks analysed here.

If we look at the activities, the cybercriminals observed cannot be easily conceptualised as OC. Indeed, many legal frameworks and criminological traditions would not cover the cybercrimes considered in this study as being OC. In countries that link OC to the seriousness of a certain criminal activity—for instance, not only the UK (see NCA 2015; Sergi 2015a) but also the international and European legal framework (Lavorgna and Sergi 2014)—many cases

considered in this study would not always meet the threshold of a minimum sentence requirement that must be met for a case to be labelled as OC.[2] In countries that target criminal enterprises instead [such as the USA with the Racketeer Influenced and Corrupt Organizations (RICO) Act] (Albanese 1996; Sergi 2015b), cybercrime is generally not recognised (yet) as one of the activities covered by anti-OC legislation.[3] If we consider criminological definitions, these have traditionally associated OC with some economic functions in that its purpose is to supply illegal goods and services (as in the case of drug trafficking), or its profit-oriented entrepreneurial nature is stressed (as in the case of money laundering) (von Lampe et al. 2006; Kleemans 2007). However, meta-analyses show that in doing so, a *quid pluris* is generally present in cases of OC, such as corruption, (threat of) violence, and attempts to gain or maintain monopoly or control over a particular criminal market (Hagan 2006; von Lampe et al. 2006). Therefore, the cybercrimes analysed would meet only the broader academic definitions, which do not consider corruption, violence, and so forth as core features of OC; they would not meet those—prevailing—definitions, according to which certain crimes might be complex and organised but still not OC if other core characteristics are missing (e.g., Finckenauer 2005).

The conceptualisation of OC as power (von Lampe 2008) stresses the systemic presence of OC, here interpreted as something more and different that simply serious crime, or crime that is organised (Lavorgna 2016): it seeks a social function through control over production and distribution of a certain commodity in the underworld, protection services, or an alliance with political and economic elites. As regards offline criminality, social functions (and sometimes even quasigovernmental features) are often attributed to OC (Potter 1994; von Lampe et al. 2006; *BKA* 2014). This aspect, however, is more problematic to recognise in cyberspace. It could be argued that in a few cases, criminal networks tried to regulate and control production and distribution of products and services via online forums: for instance, administrators and moderators can provide a certain degree of third-party enforcement over certain transactions and regulate access to forums. However, contrary to the physical world, they cannot prevent people from attempting, for example, to access the forum with another name (Lusthaus 2013). Furthermore, the existence of online forums is distinct from that of the offenders operating in it (Lusthaus 2013): even if forum administrators and moderators try to retain customers, there is no system of enforcement, no opposition against competitors, and no control over distribution.

Implications and Conclusion

The aim of this study was to investigate to what extent cybercriminals operating in phishing and malware attacks can be conceptualised as OC. To answer this question, we analysed 40 criminal networks investigated in four countries and analysed them through an OC analytical framework. The empirical analysis indicates that even if the criminal networks considered

[2] For instance, in the UK the Serious Crime Act 2015 section 45 specifies that to have an OC group the activity has to constitute an offence punishable with imprisonment for a term of 7 years or more; many of the cases considered in this study would not meet the sentencing threshold according to the 1990 Computer Misuse Act (even after it was amended by the Serious Crime Act 2015).

[3] In the USA, for instance, the RICO Act has been used to prosecute cybercriminals only in a few federal cases (Joseph 2015). In January 2015, the US Administration introduced a legislative proposal that, among other things, would expand the definition of "racketeering activity" under the RICO Act so that it applies to certain cybercrimes (see https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf), but new legislation has not passed thus far.

display the minimum set of characteristics to consider them as OC, if we only look at their structure and composition, they mostly fail to meet the existing definitions of OC when it comes to the characteristics of criminal activities carried out and social functions of these networks.

Although our analysis provided unique empirical insights to cybercrime research, it also has some limitations. Because data was gathered from people involved in the investigations, we do not have knowledge about the successful networks that so far remained undetected. In addition, all data was collected from Western countries with similar Internet access. Further research considering complementary methods (such as virtual ethnography and interviews with offenders) is needed, as is research focusing on other countries. Moreover, as we looked at cases concerning a very specific subgroup of cybercrimes, further research is needed to allow generalisability towards other types of cyber or cyber-enabled crimes (ranging from online drug trafficking to identity theft to governments and industrial espionage), which might need different organisational structures in order to be carried out effectively.

Despite these limitations, this study has important implications from both theoretical and practical perspectives. Firstly, from a theoretical perspective, it reveals some challenges in using the OC conceptualisation in cyberspace, which urges reconsideration of the capacity of our current criminological paradigms and definitions if we are to capture emerging trends in the criminal scenario (Lavorgna 2015). The whole idea behind criminalising OC in a different, more serious, way is to be found in its danger, which goes beyond the risks posed by individual offenders or occasional criminal cooperation and creates actual or potential threats to the social order (Fijnaut and Paoli 2006; Carrapico 2014). In cyberspace, however, this is no longer true, as individuals or loose associations can be as dangerous as OC (Lavorgna 2015). However, similarly to OC, the cybercrimes considered in this study (I) cause harm to a concrete victim, (II) produce systemic effects with serious consequences for society as a whole, and (III) adversely affect social control because of offenders' shielding capacity [for an assessment of the harms caused by OC, see Fijnaut et al. 1998; Kruisbergen et al. 2012; Greenfield and Paoli 2013)]. Hence, "organised"—being focus on structure, i.e., the activity or the power—has become inappropriate as a proxy indicator for seriousness or dangerousness in cyberspace. Instead, better analyses of harm, risk, and threat for specific cybercrimes are urgently needed to guide further research and theoretical developments. In addition, findings of this research suggest that further analysis addressing the relationships and the intersections between licit and illicit arenas when it comes to financial cybercrimes could be revealing.

Second, from a practical perspective, our findings question the developing narrative of cyber-OC, which—despite the lack of clear empirical evidence at times—seems to play with the ambiguity of the OC concept to make a point on the seriousness of online threats. The already exaggerated notion of OC risks have been exaggerated evenfurther: as a consequence, not only do we risk to losing its analytical and descriptive value, it will shift attention and resources from the current anti-OC efforts without a serious reflection on how to deal with new security challenges in an effective and efficient way (Lavorgna 2016). In the ongoing debate surrounding the opportunity to "adapt" the definition of OC when it comes to cyberspace, we should not uncritically embrace the logic fallacy (Hume's Law, an is-ought fallacy), according to which if a crime is "serious enough" it should be OC (Sergi 2015a). Rather, we hope that this article stimulates further debate on whether it is worthwhile to label certain cybercrimes as being OC—despite the problems outlined above—in order to

give law enforcement enhanced investigative powers or whether it would be better to address cybercrimes in an ad hoc way, for specific cybercrimes, giving different (more powerful) investigative powers and resources to investigative and analytical teams without the need to rely on the anti-OC regulatory frameworks.

References

Adamoli, S., Di Nicola, A., Savona, E.U., & Zoffi, P. (1998). *Organised Crime around the World*. Publication Series N. 31. Helsinki: Heuni.

Albanese, J. S. (1996). *Organized crime in America*. Cincinnati: Anderson Publishing.

Albanese, J. S., Das, D. K., & Verma, A. (Eds.). (2003). *Organized crime. World perspectives*. Upper Saddle River: Pearson Education.

Allum, F., Longo, F., Irrera, D., & Kostakos, P. (Eds.). (2010). *Defining and defying organised crime: Discourse, perceptions and reality*. London: Routledge.

Arsovska, J. (2011). Conceptualizing and studying organized crime in a global context. Possible? Indispensable? Superfluous? In C. J. Smith, S. X. Zhang, & R. Barberet (Eds.), *Routledge handbook of international criminology*. Abingdon: Routledge.

Birk, D., Gajek, S., Grobert, F., & Sadeghi, A.R. (2007). Phishing phishers. Observing and tracing organized cybercrime. Second International Conference on Internet Monitoring and Protection (ICIMP), doi: 10.1109/ICIMP.2007.33.

BKA (2014). *Organised Crime. National Situation Report 2014*. Bundeskriminalamt, Wiesbaden.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organization and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1–20.

Carrapico, H. (2014). Analysing the European Union's responses to organized crime through different securitization lenses. *European Security, 23*(4), 601–661.

Choo, K. K. R., & Smith, R. G. (2007). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology, 3*(1), 37–59.

Choo, K.K.R., Smith, R.G., & McCusker, R. (2007). Future directions in in technology-enabled crime. *Research and Public Policy Series* 78. Camberra*:* Australian Institute of Criminology.

Cabinet Office & Detica (2011). The cost of cybercrime. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

Edwards, A., & Levi, M. (2008). Researching the organization of serious crimes. *Criminology and Criminal Justice, 8*(4), 363–388.

Fijnaut, C. J. C., & Paoli, L. (2006). Organised crime and its control policies. *European Journal of Crime, Criminal Law and Criminal Justice, 14*(3), 307–327.

Fijnaut, C., Bovenkerk, F., Bruinsma, G., & Van de Bunt, H. (1998). *Organised crime in the Netherlands*. The Hague: Kluwer Law International.

Finckenauer, J. O. (2005). Problems of definition: what is organized crime? *Trends in Organized Crime, 8*(3), 63–83.

Finklea, K.M. (2010). *Organized crime in the United States: Trends and issues for Congress*. Congressional Research Service R40525.

Grabosky, P. (2007). The internet, technology, and organized crime. *Asian Criminology, 2*, 145–161.

Grabosky, P. (2015). Organized cybercrime and national security. In R. G. Smith, R. Chak-Chung Cheung, & L. Yiu-Chung Lau (Eds.), *Cybercrime risks and responses. Eastern and Western perspectives* (pp. 67–80). New York: Palgrave Macmillan.

Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *The British Journal of Criminology, 53*(5), 864–885.

Hagan, F. E. (2006). "Organized crime" and "organized crime": indeterminate problems of definition. *Trends in Organized Crime, 9*(4), 127–237.

Hassan, R. (2008). *The Information Society: Cyber Dreams and Digital Nightmares*. Robert Hassan. Cambridge: Polity.

Hobbs, D. (2013). *Lush life: Constructing organized crime in the UK*. Oxford: Oxford University Press.
Holt, T. K. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165–177.
Holt, T. K., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.
Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 62*(1), 1–20.
Joseph, S. W. (2015). Dismantling the internet mafia: RICO's applicability to cyber crime. *Rutgers Computer and Technology Law Journal, 41*, 268–297.
Kleemans, E. R. (2007). Organized crime, transit crime, and racketeering. *Crime and Justice. A Review of Research, 35*, 163–215.
Kleemans, E. R. (2014). Organized crime research: Challenging assumptions and informing policy. In J. Knutsson & E. Cockbain (Eds.), *Applied police research: Challenges and opportunities. Crime science series* (pp. 57–67). Cullompton: Willan Publishing.
Kleemans, E. R., & Van de Bunt, H. (1999). The social embeddedness of organized crime. *Transnational Organized Crime, 5*(1), 19–36.
Kruisbergen, E.W., van de Bunt, H.G, & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit* [Organised Crime in the Netherlands. Fourth report of the Organized Crime Monitor]. The Hague: Boom Lemma.
Kshetri, N. (2010). *The global cybercrime industry. Economic, institutional and strategic perspectives*. New York: Springer.
Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security, 45*, 58–74.
Lastdrager, E.H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(9).
Lavorgna, A. (2015). Organised crime goes online: realities and challenges. *Journal of Money Laundering Control, 18*(2), 153–168.
Lavorgna, A. (2016). Exploring the cyber-organised crime narrative: The hunt for a new bogeyman? In P. C. van Duyne (Ed.), *Organising fears, crime & law enforcement new horizons and trends in Europe & beyond*. Oisterveijk: Wolf Legal Publishers.
Lavorgna, A., & Sergi, A. (2014). Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis an in the use of Internet technologies. *International Journal of Law, Crime and Justice, 42*(1), 16–32.
Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging "cyber-organised crime" rhetoric in the United Kingdom. *International Journal of Cyber Criminology* (forthcoming).
Lavorgna, A., Lombardo, R., & Sergi, A. (2014). Organized crime in three regions: comparing the Veneto, Liverpool, and Chicago. *Trends in Organized Crime, 16*(3), 265–285.
Leukfeldt, R. (2015). Organised cybercrime and social opportunity structures: a proposal for future research directions. *The European Review of Organised Crime, 2*(2), 91–103.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016a). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. doi:10.1093/bjc/azw009.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016b). A typology of cybercriminal networks: from low tech locals to high tech specialists. *Crime, Law and Social Change*. doi:10.1007/s10611-016-9646-2.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016c). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*. doi:10.1007/s10611-016-9647-1.
Levi, M. (2014). Thinking about organised crime. Structure and threat. *The RUSI Journal, 159*(1), 6–14.
Lombardo, R. (2012). *Organized crime in Chicago*. Chicago: University of Illinois Press.
Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*(1), 52–60.
McGuire, M. (2012). *Organised crime in the digital age*. John Grieve Centre for Policing and Security and BAE Systems Detica.
NCA. (2015). *National strategic assessment of serious and organised crime 2015*. London: National Crime Agency.
Paoli, L. (2002). The paradoxes of organized crime. *Crime, Law and Social Change, 37*(1), 51–97.
Potter, G. W. (1994). *Criminal organizations. Vice, racketeering, and politics in an American City*. Prospect Heights: Waveland Press.
Schelling, T. (1971). What is the business of OC? *Journal of Public Law, 20*(1), 71–84.

Sergi, A. (2015a). Divergent mind-sets, convergent policies. Policing models against organised crime in Italy and in England within international frameworks. *European Journal of Criminology, 12*(6), 658–680.

Sergi, A. (2015b). Organised Crime in English Criminal Law, Lessons from the United States on conspiracy and enterprise corruption. *Journal of Money Laundering Control*, 18(2).

Smith, R.G. (2010). The development of cybercrime. In R. Lincoln, & S. Robinson (Eds.), *Crime over time: Temporal perspectives on crime and punishment in Australia*. Newcastle upon Tyne: Cambridge Scholars Publishing.

Tilley, N., & Hopkins, M. (2008). Organized crime and local businesses. *Criminology and Criminal Justice, 8*, 443–459.

van Duyne, P. C. (1995). The phantom and threat of organized crime. *Crime, Law and Social Change, 24*(4), 341–377.

van Duyne, P. C. (2004). Fears, naming and knowing: An introduction. In P. C. van Duyne, M. Jager, K. von Lampe, & J. L. Newell (Eds.), *Threats and phantoms of organised crime, corruption and terrorism* (pp. 1–21). Nijmegen: Wolf Legal Publishers.

van Duyne, P. C., & Nelemans, M. D. H. (2012). Transnational organized crime: Thinking in and out of Plato's Cave. In A. Felia & S. Gilmour (Eds.), *Routledge handbook of transnational organized crime* (pp. 36–51). London: Routledge.

Varese, F. (2010). What is organised crime? In F. Varese (Ed.), *Organised crime: Critical concepts in criminology* (pp. 1–33). New York: Routledge.

von Lampe, K. (2008). Organized crime in Europe: conceptions and realities. *Policing* (2)1, 7–17.

von Lampe, K., Van Dijck, M., Hornsby, R., Markina, A., & Verpoest, K. (2006). Organized Crime is…: Findings from a cross-national review of literature. In P. C. Duyne, A. Maljevic, M. Van Dijck, K. von Lampe, & J. L. Newell (Eds.), *The organization of crime for profit: Conduct, law and measurement.* Nijmegen: Wolf Legal Publishers.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.

Wall, D. (2008). Cybercrime, media, and insecurity. The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology, 22*(1–2), 45–63.

Wall, D. (2015). Dis-organised crime: towards a distributed model of the organisation of cybercrime. *The European Review of Organised Crime, 2*(2), 71–90.

Williams, Ph. (2001). Organized crime and cybercrime: Synergies, trends, and responses. *Arresting Transnational Crime. An Electronic Journal of the U.S. Department of State*, 6(2).

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Journal of Policing and Society, 23*(4), 516–539.